

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION ASSOCIATED WITH
LOVEJOYBABY@ICLOUD.COM,
MORGANCALDWELL1517@GMAIL.COM, and
PAULDEMARCOS10@PROTONMAIL.COM, STORED AT PREMISES
CONTROLLED BY APPLE INC.

)
Case No. 21-MJ-704-JFJ
)
)
)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):*

See Attachment "B"

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

10/13/21

(not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

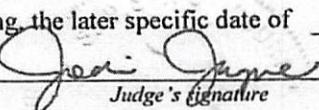
Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box):

for _____ days *(not to exceed 30).*

until, the facts justifying the later specific date of _____.

Date and time issued:

9/30/21, 3:59pm


Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return	<i>Submitted To</i>	
Case No.: <i>21-MJ-704-JFJ</i>	Date and time warrant executed: <i>30 Sept 2021 @ 1647</i>	Copy of warrant and inventory left with: <i>Apple Inc.'s Legal Portal</i>
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized: <i>2x emails from Apple containing Encrypted DATA + Decryption Keys.</i>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: <u>15 Oct 2021</u></p> <p> _____ <i>Brian S. Dean</i> Executing officer's signature</p> <p><u>SA BRIAN S. DEAN</u> Printed name and title</p>		

ATTACHMENT A - PROPERTY TO BE SEARCHED

This warrant applies to information associated with

LOVEJOYBABY@ICLOUD.COM,

MORGANCALDWELL1517@GMAIL.COM, and

PAULDEMARCO510@PROTONMAIL.COM (Target Accounts 1-3) stored at

premises owned, maintained, controlled, or operated by Apple Inc., a company

headquartered at Apple Inc., One Apple Park Way, Cupertino, California, 95014.

ATTACHMENT B – ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”),

Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from August of 2019 through present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August of 2019 through present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud account from August of 2019 through present, including all iOS device backups, all Apple

and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers) account from August of 2019 through present, including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations account from August of 2019 through present where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple account from August of 2019 through present and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes as fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2422 (Coercion and Enticement), 18 U.S.C. §§ 2251(a) (Sexual Exploitation of Children), 18 U.S.C. § 2252(a)(2)(A) and (B) (Receipt of Child Pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence indicating other accounts used by the owner of the Apple ID
- b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.